PREVENTING ID SPOOFING WITH UBIQUITOUS SIGNATURE CERTIFICATES

ABSTRACT OF THE DISCLOSURE

A technique for preventing ID spoofing by hackers with ubiquitous signature certificates includes allowing a user to access a registration server. Upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server queries a directory to obtain information regarding the identified user. Upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informs the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate. Furthermore, upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informs the user that a signature certificate will not be issued.